REMARKS

The Office Action dated December 16, 2004 has been received and carefully considered. In this response, the specification, figures and claims 1, 3-5, 7, 9, 11, 12, 16 and 25 have been amended to provide proper antecedent support and to correct various informalities such as by removing unnecessary "step of" language. Claims 6, 14, 18 and 28 have been canceled and claims 33-35 have been added. The amendments to the claims do not narrow the scope of the claims and support for the amendments to the specification, figures and claims and the addition of claims may be found in the specification and figures as originally filed. Reconsideration of the outstanding objections and rejections therefore is respectfully requested in view of the following remarks.

Telephonic Interview of March 2, 2005

The undersigned notes with appreciation the courtesies extended by the Examiner during the telephonic interview of March 2, 2005. During this interview, the Applicant's representative and the Examiner discussed the references with regard to the claims limitations of generating two encrypted streams from a single encrypted stream. As agreed to by the Examiner, these claim limitations, in addition to the clarification that the claimed data streams are digital data streams, would overcome the rejections of the claims in view of the cited references. The Applicant has amended the claims accordingly.

Objection to the Drawings

At page 2 of the Office Action, Figure 1 was objected to as including a reference character (element 125) not mentioned in the specification. The specification has been amended to include reference to element 125. Withdrawal of this objection therefore is respectfully requested.

At page 2 of the Office Action, Figure 5 was objected to as failing to comply with 37 C.F.R. Section 1.84(g) and p(3) due to the margins of Figure 5 and the presence of reference characters that are less than 1/8" tall or that overwrite dotted lines. Figure 5 has been replaced by Replacement Figures 5A and 5B (attached hereto as Appendix A) in view of the Examiner's remarks and the specification has been amended accordingly. No new matter is introduced by

Replacement Figures 5A and 5B. Entry thereof and withdrawal of the objection to Figure 5 therefore is respectfully requested.

Objection to the Specification

At page 3 of the Office Action, the specification was objected to for lacking a Brief Summary of the Invention. It is respectfully submitted that no Brief Summary of the Invention section is to be provided, as allowed by the suggestive language of 37 C.F.R. Section 1.77(b) requesting, but not requiring, said summary.

The specification also was objected to for including multiple references to an enclosed document "Upstream link for HDCP Revision 0.95" which the Examiner asserts is not found in the application. The Applicant has amended the specification to remove the "enclosed" language. A copy of the identified document is submitted herewith in an Information Disclosure Statement. Withdrawal of this objection therefore is respectfully requested.

Objection to Claim 11

At page 3 of the Office Action, claim 11 was objected to for being unclear. Claim 11 has been amended consistent with the Examiner's remarks. The amendments to claim 11 do not narrow the scope of claim 11. Withdrawal of this objection therefore is respectfully requested.

Rejection of Claims 6, 14, 18 and 28

At page 4 of the Office Action, claims 6, 14, 18 and 28 were rejected under 35 U.S.C. Section 112, first paragraph. Claims 6, 14, 18 and 28 have been canceled without prejudice, thereby obviating this rejection. Withdrawal of this rejection therefore is respectfully requested.

Rejection of Claims 3 and 7

At page 5 of the Office Action, claims 3 and 7 were rejected under 35 U.S.C. Section 112, second paragraph. Claims 3 and 7 have been amended consistent with the Examiner's remarks. The amendments to claims 3 and 7 do not narrow the scope of the claims. Withdrawal of this rejection therefore is respectfully requested.

Anticipation Rejection of Claim 1

At page 6 of the Office Action, claim 1 was rejected under 35 U.S.C. Section 102(b) as being anticipated by Katznelson (U.S. Patent No. 5,091,936). This rejection is respectfully traversed.

Claim 1 presently recites the limitations of receiving a single data stream, encrypting a first portion of the single digital data stream with a first encryption key to generate a first encrypted stream and encrypting a second portion of the single data stream with a second encryption key to generate a second encrypted stream. With respect to these limitations, the Examiner asserts that "Katznelson discloses the encrypting of portions of a data stream, such as video and audio, each using encryption algorithms (see column 6, lines 23-35)." The relied-upon passage of Katznelson is provided below:

> *Insertion of the encrypted audio* into the horizontal blanking interval is provided by waveform multiplexer 36, which *combines* the audio data with the scrambled video from video processor 32 or a multiplexed plurality of digital audio/data signals from audio processors 24, 26, . . . 28. Waveform multiplexer 36 also receives a video mode reference or audio mode reference pattern from reference pattern selector 44, as well as burst data and control channel data from burst generator 46 and control channel processor 48, respectively. All of the various signals coupled to waveform multiplexer 36 *are combined into a composite waveform output from the multiplexer for transmission to a receiver.*

Katznelson, col. 6, lines 23-35 (emphasis added).

As a first issue, it is respectfully submitted that the Examiner characterizes the above cited passage of Katznelson as disclosing "the encrypting of portions of a data stream, such as video and audio, each using encryption algorithms," but fails to address the encryption of one portion of a data stream using a first encryption key and the encryption of a second portion of the data stream using a second encryption key as recited by claim 1. *See Office Action*, p. 6. Moreover, the Examiner fails to address how Katznelson discloses the limitations of the first portion of the data stream being encrypted *to generate a first encrypted stream* and the limitations of the second portion of the data stream being encrypted *to generate a second encrypted stream* as recited by claim 1. In fact, the Examiner admits that Katznelson fails to disclose "the separating of the video stream into separate streams . . ." and therefore consequently inherently admits that Katznelson fails to disclose the limitations of encrypting first and second portions of a data stream to generate first and second encrypted streams, respectively, as recited by claim 1. *See Id.*, p. 8.

Moreover, the Applicant respectfully submits that the above-cited passage of Katznelson fails to disclose encrypting any portion of a data stream. Instead, the above-cited passage of Katznelson merely discloses that encrypted audio and scrambled video are *combined by the waveform multiplexer 36 into a composite waveform. Id.* Accordingly, while Katznelson discloses combining encrypted/scambled data to generate a combined waveform, claim 1, in sharp contrast, recites the limitations of encrypting the first and second portions of a single data stream to generate first and second encrypted streams. The above-cited passage of Katznelson fails to disclose encrypting first and second portions of a single data stream using first and second encryption keys, respectively, as recited by claim 1. Consequently, the above-cited passage of Katznelson necessarily fails to disclose that the first and second portions are encrypted to generate first and second encrypted streams, respectively, as recited by claim 1. Accordingly, the Office Action fails to establish that Katznelson discloses each and every limitation of claim 1.

In view of the foregoing, it is respectfully submitted that the anticipation rejection of claim 1 is improper at this time and withdrawal of this rejection therefore is respectfully requested.

Anticipation Rejection of Claims 12, 20, 25 and 31

At page 6 of the Office Action, claims 12, 20, 25 and 31 were rejected under 35 U.S.C. Section 102(b) as being anticipated by Katznelson and Gilhousen (U.S. Patent No. 4,613,901). This rejection is respectfully traversed.

Claim 12, from which claim 20 depends, presently recites the limitations of a cipher component capable of receiving a single digital data stream, applying the first encryption key to a first portion of the digital data stream, and applying the second encryption key to a second portion of the digital data stream. In rejecting claim 12 (as well as claim 25, discussed below), the Office Action relies on Katznelson as applied to claim 1 (discussed above) and further on the disclosure of Gilhousen. *Office Action*, p. 6. As noted above with respect to claim 1, Katznelson fails to disclose encrypting first and second portions of a data stream. Katznelson therefore fails to disclose a cipher component capable of applying a first encryption key to a first portion of a data stream and applying a second encryption key to a second portion of the data stream as recited by claim 12. The Office Action does not assert that Gilhousen discloses these limitations. *Id.* Accordingly, it is respectfully submitted that the Office Action fails to establish that the proposed combination of Katznelson and Gilhousen discloses or suggests each and every limitation of claim 12, as well as each and every limitation of claim 20 at least by virtue of its dependency from claim 12. Moreover, claim 20 recites additional limitations neither disclosed nor suggested by the cited references.

Claim 25, from which claim 31 depends, recites the limitations of a first decryption component capable of decrypting a first link of encrypted data, using a first encryption key, to generate a first portion of a single received digital data stream and a second decryption component capable of decrypting a second link of encrypted data, using a second encryption key, to generate a second portion of the received digital data stream. The relied-upon passage of Katznelson does not disclose nor suggest decrypting first and second links of encrypted data using first and second encryption keys as recited by claim 1, nor does the relied-upon passage of Katznelson disclose or suggest that the first and second links of encrypted data are decrypted to generate first and second portions of a single received data stream as recited by claim 25. The Office Action does not assert that Gilhousen discloses at least these limitations. Accordingly, it is respectfully submitted that the Office Action fails to establish that the proposed combination of Katznelson and Gilhousen discloses or suggests each and every limitation of claim 25, as well as each and every limitation of claim 31 at least by virtue of its dependency from claim 25. Moreover, claim 31 recites additional limitations neither disclosed nor suggested by the cited references.

In view of the foregoing, it is respectfully submitted that the anticipation rejection of claims 12, 20, 25 and 31 is improper at this time and withdrawal of this rejection therefore is respectfully requested.

Anticipation Rejection of Claims 1-4

At page 7 of the Office Action, claims 1-4 were rejected under 35 U.S.C. Section 102(e) as being anticipated by Wright (U.S. Patent No. 6,052,466). This rejection is respectfully traversed.

Claim 1, from which claims 2-4 depend, presently recites the limitations of receiving a single digital data stream, encrypting a first portion of the single data stream with a first encryption key to generate a first encrypted stream and encrypting a second portion of the single data stream with a second encryption key to generate a second encrypted stream. With respect to claim 1, the Examiner states that "Wright discloses a system wherein a single data stream is divided into at least two cipher streams, each respectively using a generated key (see column 5, line 58 to column 6, line 45)." *Office Action*, p. 7. For ease of reference, the relied-upon passage of Wright is provided:

> The key generators 116 of the security devices 112 for Party A and Party B now independently generate a shared private key K in accordance with Equations (4) and (5), respectively. While the security devices 112A and 112B are able to independently generate the same private key K, it will be recognized that an eavesdropper is unable to compute the private key, in spite of having access to the public keys PK_A and PK_B, because knowledge of the secret random quantities x and y is unknown and cannot be mathematically determined. The private keys K are then applied to initialize the first cipher stream generators 120 *which output a first ciphe r stream C.*
>
> This first cipher stream C is then processed by the partition and index device 121 *which partitions the cipher stream into a sequence of secondary private keys C_1, C_2, . . . , C_i. The sequence of secondary private keys C_1, C_2, . . . , C_i is then applied to initialize the second cipher stream generators 123 which output a second cipher stream C'. This second cipher stream C' is then either exclusively ORed 122 with the plaintext sequence (PT) to generate ciphertext (CT) for transmission over the channel 111, or exclusively ORed with received ciphertext to generate plaintext.* Each secondary private key C_i is further provisioned by the device 121 with a uniquely identifying index. The index indicating which secondary private key C_i is being used to encrypt a particular plaintext sequence PT_i is communicated over the channel 111 to ensure synchronization and the utilization of the correct key for decryption. This index may be exchanged between the security devices 112 in un-encrypted form because it bears no information concerning the secondary private key C_i other than a sequence (i.e., indexing) number.
>
> Reference is now made to FIG. 4 wherein there is shown a flow diagram for secondary private key generation. For a bi-directional data communication between Party A and Party B as illustrated in FIG. 3, the private key K actually comprises (i.e., may be split into) two keys K_{AB} and K_{BA}. *The need for two private keys when handling bi-directional communications is required to ensure that the same cipher stream is never used for the encryption of different plaintext sequences. The first private key K_{AB} is used to generate a forward first cipher stream C_{AB}, and the second private key K_{BA} is used to generate a reverse first cipher stream C_{BA}.* The forward first cipher stream C_{AB} is then partitioned and

> indexed to generate a first (or forward channel) secondary private key C_{ABi} sequence, with individual ones in the sequence used to generate a forward second cipher stream C_{AB}' that is used by security device 112A to encrypt Party A PT_i data communications, and by security device 112B to decrypt Party A CT_i data communications. The reverse first cipher stream C_{BA}, on the other hand, is then partitioned and indexed to generate a second (or reverse channel) secondary private key C_{BAi} sequence, with individual ones in the sequence used to generate a reverse second cipher stream C_{BA}' that is used by security device 112B to encrypt Party B PT_i data communications, and by security device 112A to decrypt Party B CT_i data communications.

Wright, col. 5, line 57 to col. 6, line 45 (emphasis added).

The Applicant respectfully submits that the Examiner has mischaracterized the disclosure of Wright. As the above relied-upon passage illustrates, Wright teaches a technique whereby a private key K is used to create a cipher stream C of secondary private keys $C_1, C_2, \ldots C_i$ that are then used to encrypt data packets sent from one "Party" to another "Party." *Id.* Wright discloses that the "second cipher stream C' [derived from cipher stream C] is exclusively ORed 122 with the plaintext sequence (PT_i) to generate ciphertext (CT_i) . . . ." *Id.*, col. 6, lines 8-10. Accordingly, Wright teaches that each element i of a plaintext sequence is XORed with the corresponding private key C_i to generate a ciphertext element CT_i. *Id., see also Id*, Abstract. Thus, while Wright discloses that XORing different elements of the plaintext sequence using different private keys to generate ciphertext, Wright does not teach that encrypting the plaintext results in first and second encrypted streams and therefore fails to disclose the limitations of encrypting a first portion of a data stream to generate a first encrypted stream and encrypting a second portion of the data stream to generate a second encrypted stream as recited by claim 1. Accordingly, Wright fails to disclose each and every limitation of claim 1, as well as each and every limitation of claims 2-4 at least by virtue of their dependency from claim 1.

Furthermore, claims 2-4 recite additional limitations are not disclosed by Wright. For example, claim 4 recites the limitations of receiving the first and second encrypted streams, decrypting the first encrypted stream to generate a first portion of a received data stream, decrypting the second encrypted stream to generate a second portion of the received data stream, and combining the first portion of the received data stream with the second portion of the received data stream to generate a single received data stream. As Wright fails to disclose the generation of both a first and second encrypted stream, Wright necessarily fails to disclose receiving the first and second encrypted streams as recited by claim 4. Additionally, Wright fails to disclose the decryption of first and second encrypted streams to generate a first portion and a second portion, respectively of a received data stream and the combining of the first and second portions to generate a single received data stream as recited by claim 4.

In view of the foregoing, it is respectfully submitted that the anticipation rejection of claims 1-4 is improper at this time and withdrawal of this rejection therefore is respectfully requested.

Obviousness Rejections of Claims 4-11, 13-19, 21-24, 26-30 and 32

At page 8 of the Office Action, claims 4, 9-11, 13-16, 26 and 30 were rejected under 35 U.S.C. Section 103(a) as being unpatentable over Katznelson in view of Butler (U.S. Patent No. 6,597,402) and claims 5, 6, 17, 18, 27 and 28 were rejected under 35 U.S.C Section 103(a) as being unpatentable over Katznelson in view of Butler and further in view of Bartulis (U.S. Patent No. 4,332,464). At page 9 of the Office Action, claims 7, 8, 19 and 29 were rejected under 35 U.S.C. Section 103(a) as being unpatentable over Katznelson in view of Butler and Bartulis and further in view of Posner (U.S. Patent No. 4,389,671). At page 10 of the Office Action, claims 21 and 32 were rejected under 35 U.S.C. Section 103(a) as being unpatentable over Katznelson and Gilhousen in view of Otera (U.S. Patent No. 6,507,346) and claims 22-24 were rejected under 35 U.S.C. Section 103(a) as being unpatentable over Katznelson and Gilhousen in view of Otera and further in view of DDWG (Digital Display Working Group, DVI Specification 1.0). These rejections are respectfully traversed.

Claim 1, from which claims 4-11 depend, recites the limitations of encrypting a first portion of a digital data stream to generate a first encrypted stream and encrypting a second portion of the data stream to generate a second encrypted stream. As noted above, Katznelson fails to disclose or suggest these limitations. The Office Action does not assert that any of Butler, Bartulis, Gilhousen, Otera or DDWG discloses or suggests these limitations. Accordingly, the Office Action fails to establish that any of the proposed combinations of Katznelson, Butler, Gilhousen, Barulis, Otera and DDWG discloses or suggests each and every limitation of claims 4-11 at least by virtue of their dependency from claim 1.

Moreover, claims 4-11 recite additional limitations neither disclosed nor suggested by the cited references. To illustrate, claim 10 recites the additional limitations of wherein the first portion of the single data stream is associated with even pixels and the second portion of the single data stream is associated with odd pixels. With respect to these limitations, the Examiner asserts that

> Butler discloses the splitting (and later recombining) of a video stream into separate data streams, placing even pixels into one stream and odd pixels into the other. Butler also discloses the use of a "line doubler," which ensures that each of the two (odd and even) streams transmits at half the throughput of the video stream (see column 10, line 53 to column 11, line 15), and further suggests that line doubling reduces visible line structure (see column 1, lines 35-37). The line double uses a half speed clock in its operation.

Office Action, p. 8.

Based on this characterization of the disclosure of Butler, the Examiner reasons that "it would have been obvious . . . to modify the invention of Katznelson by separating the stream into even and odd pixel streams and using line doubling, as disclosed by Butler, as that [sic] line doubling reduces visible line structure." *Id.*

As noted above, Katznelson fails to disclose encrypting first and second portions of a single data stream to generate first and second encrypted streams, respectively, as recited by claim 1 (from which claim 10 depends), so the proposed combination of Katznelson and Butler would fail to disclose or suggest each and every limitation of claim 11. However, even if it is assumed, *arguendo*, that Katznelson disclosed these limitations, the Applicant respectfully submits that one of ordinary skill in the art would find no motivation to combine the teachings of Katznelson and Butler, the Examiner's reasons notwithstanding. The disclosure of Butler is drawn to reducing the visible line structure and flicker in video displays by increasing the field rate and the number of lines. *See Butler*, Title and Abstract. The disclosure of Katznelson is drawn to the transmission of digital audio content or other digital data during the horizontal blanking interval of a video signal, where the digital audio data may scrambled for security. *See Katznelson*, Abstract and col. 1, line 52 to col. 2, line 22. Katznelson provides no disclosure related to the display of the video signal and therefore provides no suggestion that reduced flicker and visible line structure would be desirable. Butler provides no disclosure related to the reception of digital audio data and therefore provides no suggestion that receiving digital audio data during a vertical blanking interval would be desirable. Although the Examiner concludes that one of ordinary skill in the art would be motivated to modify Katznelson "by separating the stream into even and odd pixel streams and using line doubling" because "line doubling reduces visible line structure," the Examiner fails to explain how the digital audio data provision technique taught by Katznelson would benefit from the technique for reducing visible line structure as taught by Butler. Conversely, the Examiner fails to explain how the visible line structure reducing technique taught by Butler would benefit from the digital audio data provision technique taught by Katznelson. Accordingly, as the system of Katznelson provides no suggestion that the teachings of Butler would be useful, and *vice versa*, one of ordinary skill in the art would not be motivated to combine the teachings of Katznelson and Butler as proposed by the Examiner. The Applicant therefore respectfully submits that the Office Action fails to establish a*prima facie* case of obviousness for claim 10.

As another example, claim 15, which depends from claim 12, recites the additional limitations of wherein the cipher component applies the first encryption key to even bits in the single data stream and applies the second encryption key to odd bits in the single data stream. The Office Action asserts that the proposed combination of Katznelson and Butler disclose at these limitations. The Applicant respectfully submits that neither Katznelson nor Butler disclose encrypting even bits of a data stream using one key and encrypting odd bits of a data stream using a second key as recited by claim 15. Moreover, the Office Action fails to address how either of Katznelson or Butler disclose these limitations. It therefore is respectfully submitted that the Office Action fails to establish that the proposed combination of Katznelson and Butler discloses or suggests each and every limitation of claim 15.

In view of the foregoing, it is respectfully submitted that the obviousness rejection of claims 4-11, 13-19, 21-24, 26-30 and 32 are improper at this time and withdrawal of these rejections therefore is respectfully requested.

Addition of Claims 33-35

New claims 33-35 have been added. Support for the addition of new claims 33-35 may be found in the specification and drawings as originally filed. No new matter is introduced by new claims 33-35. The Applicant respectfully submits that none of the cited references disclose or suggest, alone or in combination, the each and every limitation of claims 33-35 for at least the reasons provided above with respect to claims 10 and 15.

Conclusion

It is respectfully submitted that the present application is in condition for allowance, and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number in order to expedite resolution of any issues and to expedite passage of the present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

Applicants do not believe that any additional fees are due, but if the Commissioner believes additional fees are due, the Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 50-0441.

Respectfully submitted,

16 March 2005
Date

Ryan S. Davidson, Reg. No. 51,596
on behalf of
J. Gustav Larson, Reg. No. 39,263,
Attorney for Applicant
TOLER, LARSON & ABEL, L.L.P.
5000 Plaza On The Lake, Suite 265
Austin, Texas 78746
(512) 327-5515 (phone) (512) 327-5452 (fax)

IN THE DRAWINGS:

Please replace Figure 5 with the Replacement Figures 5A and 5B attached as Appendix A.

APPENDIX A